AMENDED SPECIFICATION

➢ **Replace the paragraph starting at page 4, line 8 with the following:**

As a result of shortcomings in the above-referenced fraud reduction techniques, non-authorized users may be able to use stolen or otherwise improperly obtained data cards and authorization codes as if the non-authorized user was in fact an authorized user. As long as verification systems are based solely on data that is easily replicated and transferred—as opposed to data that is irreproducible and unique to an authorized user—such systems must rely, at least in part, on the authorized user's diligence and often luck in secreting some part of the data card. Recent increases in data card scams and automated teller machine ("ATM") infractions, for example, testify to the vulnerability of such data card systems, as do complaints from authorized ~~user's~~ users who unwisely or unknowingly tendered a data card to a less thrifty friend or family member. Thus, what is needed are methods and systems for allowing secure data card transactional activity, thereby eliminating or reducing fraud in connection therewith.

➢ **Replace the paragraph starting at page 5, line 5 with the following:**

Biometric verification systems are ordinarily implemented by measuring or recording a referent biocharacteristic from an authorized user to be used for future comparisons. Then, in every subsequent access attempt, a sampled live biocharacteristic is compared against the referent master biocharacteristic in an attempt to verify the possessor's identity as an authorized user. Because the biocharacteristic is uniquely personal to the authorized user, and because the act of physically presenting the biocharacteristic is virtually irreproducible, biocharacteristic matches are putative of actual identity—as opposed to verifying identity by possession of a freely-transferable data card or authorization code—and thereby ~~reducing~~ reduce fraud, for example, by deterring a false affidavit claiming a data card was stolen or that its use was not otherwise authorized. What is needed, therefore, are improvements in the versatility of existing biometric verification systems.

➢ **Replace the paragraph starting at page 6, line 11 with the following:**

Reference is also made to the following applications, filed herewith and hereby incorporated by reference: Method and System for Interacting with a Biometric Verification System, U.S. Pat. App. No. 09/828,069 to inventors Dustin M. Davis and Jane R. Garrison; Method and System for Consummating a Transaction in a Biometric Verification System Based on Prior Transactional Histories, U.S. Pat. App. No. 09/828,497 to inventors Dustin M. Davis

and Jane R. Garrison; and Method and System for Migrating Dynamic Master Templates in a Biometric Verification System, U.S. Pat. App. No. 09/828,597 to inventors Garland R. Bullock and Paul V. Tischler.

➢ **Replace the paragraph starting at page 10, line 3 with the following:**

The biometric scanning device 16 and other periphery 18 connect to the control terminal 14 by well-known interfacing techniques for connecting serial devices, such as RS-485, RS-232, Universal Serial Bus ("USB"), and other standard interfaces. However, the present invention is not limited to any of these standard interfaces, nor to any other of the above-described arrangements. For example, the biometric scanning device 16 may not connect to the control terminal 14 in a second representative point-of-sale 12b, or a third representative point-of-sale 12c may comprise only the biometric scanning ~~16~~ device 16, which, in turn, may comprise a biometric scanner 26 other than the one described above. In addition, the alphanumeric data input device 20 and textual and graphic output device 24 may be combined into a single device using a light pen, mouse, pull-down menus, or other well-known techniques for data input and output.

➢ **Replace the paragraph starting at page 10, line 14 with the following:**

With the environment 10, a central server ("CS") 28 preferably connects to the points-of-sale 12 to establish client-server relationships therewith. The CS 28 preferably connects to the points-of-sale 12 by the well-known Transmission Control Protocol ("TCP") and Internet Protocol ("IP"), or if the ~~second~~ third representative point-of-sale 12c comprises only the biometric scanning device 16, then by the TCP/IP, RS-485, short range radio, or other standard interfaces. A representative CS 28 includes, for example, a PENTIUM® class machine available from Dell Computer Corporation of Austin, Texas. Physically, the CS 28 is local to or remote from the points-of-sale 12.

➢ **Replace the paragraph starting at page 29, line 15 with the following:**

From step 150, control then passes to step 154 if the system does not receive additional primary identification data; otherwise, control passes from step 150 to step 156 to store additionally received primary identification data, as previously discussed, and then back to step 150. From Step 154, control passes to steps 158 if the system does not receive additional secondary identification data; otherwise, control passes from step 154 to step 160 to store additionally received secondary identification data, as previously discussed, and then back to

step 154. The method then terminates after 158 if the system does not receive additional financial account data; otherwise, control passes from step 158 to step 162 to store additionally received financial account data, as previously discussed, and then back to step 158. With control passing through these loops, it can store additional enrollment data, primary identification data, secondary identification data, and financial account data, as desired. The system can store the modified data, if any, in the fixed storage device 34 of Fig. 1. Alternatively, the system can require receiving a specified type of identification data to modify ~~consummate transactions~~ previously stored data. For example, the system may require receiving primary identification data to change enrollment data such as an applicant's address, although the system is not limited in this regard.